

82478-4800

1Bw

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:

Takatoshi Ono et al.

Serial No.: 10/763,958

Filed: January 23, 2004

For: ELLIPTIC CURVE EXPONENTIATION
APPARATUS THAT CAN COUNTER
DIFFERENTIAL FAULT ATTACK, AND
INFORMATION SECURITY APPARATUS

Patent Examiner:

Group Art Unit: 2131

May 17, 2006

Irvine, California 92614

SUPPLEMENTAL
INFORMATION DISCLOSURE STATEMENT

Mail Stop Amendment
Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

Dear Sir:

In an attempt to fully comply with the duty of disclosure set forth in 37 C.F.R. § 1.56 and in conformance with 37 C.F.R. §§ 1.97 and 1.98, applicant wishes to bring to the attention of the U.S. Patent Office the following references, which was found during the prosecution of a co-pending European patent application:

European Patent Application No. EP 1 237 322

Antipa et al., "Validation of elliptic curve public keys", Public Key Cryptography-PKC 2003 6th International Workshop on Practice and Theory in Public Key Cryptography, 6 January 2003, pp. 211-223.

Biehl et al., "Differential Fault Attacks on Elliptic Curve Cryptosystems", Advances in Cryptology, 20th Annual International Cryptology Conference, Aug. 20-24, 2000. Proceedings, Lecture Notes in Computer Science; Vol. 1880 Berlin, Springer, DE 20 August 2000, pp. 131-146.

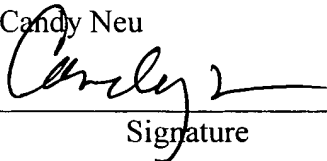
Copies of these references and form PTO-A820 are attached.

The undersigned attorney hereby certifies that each item contained in the Information Disclosure Statement was cited in a communication from a foreign patent office in a counterpart international application not more than three months prior to filing this statement.

If the Examiner believes that a telephone conference would help further the prosecution of this case, he is respectfully requested to contact the undersigned attorney at the listed telephone number.

I hereby certify that this correspondence is being deposited with the U.S. Postal Service as first class mail in an envelope addressed to: Mail Stop Amendment, Commissioner for Patent, PO Box 1450, Alexandria, VA 22313-1450 on May 17, 2006

by: Candy Neu

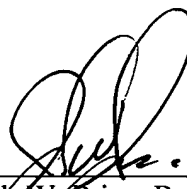


Signature

Date of Signature: May 17, 2006

Very truly yours,

SNELL & WILMER LLP



Joseph W. Price, Reg. No. 25,124
600 Anton Boulevard, Suite 1400
Costa Mesa, CA 92626-7689
Tel: 714-427-7420
Fax: 714-427-7799

INFORMATION DISCLOSURE CITATION <i>(Use several sheets if necessary)</i>				Docket Number (Optional)		Application Number		
				82478-4800		10/763,958		
				Applicant(s)				
				Takatoshi Ono et al.				
				Filing Date		Group Art Unit		
				01/23/2004		2131		
U. S. PATENT DOCUMENTS								
EXAMINER INITIAL	REF	DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE IF APPROPRIATE	
U.S. PATENT APPLICATION PUBLICATIONS								
EXAMINER INITIAL	REF	DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE IF APPROPRIATE	
FOREIGN PATENT DOCUMENTS								
	REF	DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUBCLASS	Translation	
							YES	NO
		1 237 322	04.09.2002	Europe			X	
OTHER DOCUMENTS <i>(Including Author, Title, Date, Pertinent Pages, Etc.)</i>								
		Antipa et al., "Validation of elliptic curve public keys", Public Key Cryptography-PKC 2003 6th International Workshop on Practice and Theory in Public Key Cryptography, 6 January 2003, pp. 211-223.						
		Biehl et al., "Differential Fault Attacks on Elliptic Curve Cryptosystems", Advances in Cryptology, 20th Annual International Cryptology Conference, Aug. 20-24, 2000. Proceedings, Lecture Notes in Computer Science; Vol. 1880, Berlin, Springer, DE 20 August 2000, pp. 131-146.						
EXAMINER				DATE CONSIDERED				
EXAMINER: Initial if citation considered, whether or not citation is in conformance with MPEP 609; draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.								